(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 2001067270 A

(43) Date of publication of application: 16.03.01

(51) Int. Cl G06F 12/14
G06F 9/06

(21) Application number: 11241239

(22) Date of filing: 27.08.99

(71) Applicant: NIPPON TELEGR & TELEPH CORP <NTT>

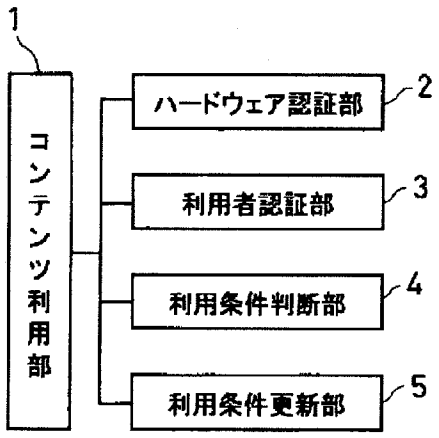
(72) Inventor: SHIONOIRI OSAMU
ISHIMARU ATSUHIKO

(54) CONTENTS SHARING MANAGEMENT SYSTEM AND CONTENTS PROTECTING METHOD AND RECORDING MEDIUM WHERE THE METHOD IS RECORDED

(57) Abstract:

PROBLEM TO BE SOLVED: To obtain a contents sharing management system allowing users to execute shared use such as the duplication of contents within the range of proper right and a contents protecting method.

SOLUTION: At the time of going to use contents in a contents using part 1, whether the hardware is proper or not, and whether the user is authorized or not is authenticated by a hardware authenticating part 2 and a user authenticating part 3 respectively at need in order to check whether the user condition is fulfilled or not. At the time of judging any one or both of the hardware and the user to be improper, a use condition judging part 4 judges whether or not the new permission of the hardware or the user is admitted as the user condition, and when they are permitted, a user condition updating part 5 updates the use condition based on one or both of the present hardware information and the user information. Thus, the contents sharing different hardware can be realized based on the proper use condition.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－67270
（P2001－67270A）
(43)公開日　平成13年３月16日(2001.3.16)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｆ	５Ｂ０１７
			３２０Ｂ	５Ｂ０７６
			３２０Ｃ	
9/06	５５０	9/06	５５０Ｇ	

審査請求　未請求　請求項の数11　ＯＬ　（全 11 頁）

(21)出願番号　特願平11－241239

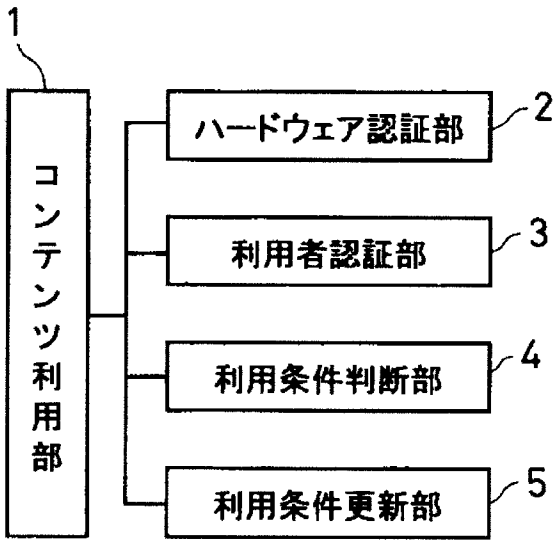
(22)出願日　平成11年８月27日(1999.8.27)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　塩野入　理
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　石丸　敦彦
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100062199
弁理士　志賀　富士弥　（外１名）

最終頁に続く

(54)【発明の名称】　コンテンツ共有管理システムおよびコンテンツ保護方法およびこの方法を記録した記録媒体

(57)【要約】
【課題】　正当な権利の範囲内において、利用者がコンテンツを複製するなど共有利用できる共有管理システム、コンテンツ保護方法を提供する。
【解決手段】　コンテンツ利用部１において、コンテンツを利用しようとした時、利用条件に沿っているか否かを調べるため必要に応じて、ハードウェア認証部２にて正当なハードウェアか否かを、利用者認証部３にて正当な利用者か否かを認証する。どちらか一方または両方が正当でないと判断した時、利用条件としてハードウェアや利用者の新たな許諾が許されているか否かを利用条件判断部４で判断し、許されているなら、利用条件更新部５において現在のハードウェア情報または利用者情報または両方を元に、利用可能とするように利用条件を更新する。これにより、正当な利用条件の基に、異なるハードウェアでのコンテンツ共有等を可能にする。



1

【特許請求の範囲】

【請求項１】　ディジタルコンテンツ流通における、コンテンツ共有管理システムであって、

コンテンツに指定されたコンテンツ利用条件または更新された利用条件に基づきコンテンツを利用するコンテンツ利用部と、

コンテンツの利用ハードウェアが正当かどうかを認証するハードウェア認証部と、

コンテンツの利用者が正当かどうかを認証する利用者認証部と、

前記認証の結果、正当な利用者による他のハードウェア上での利用、または、正当なハードウェア上での他の利用者による利用である場合には、その利用がそのコンテンツにおいて許されているか否かを調べる利用条件判断部と、

前記判断の結果、許されている場合には、コンテンツの利用条件を利用可能とするように更新する利用条件更新部とを、

有することを特徴とするコンテンツ共有管理システム。

【請求項２】　前記コンテンツ利用条件に、あらかじめ複数の利用ハードウェア情報または複数の利用者情報を登録する機能手段を有し、

前記ハードウェア認証部または前記利用者認証部は、コンテンツの利用ハードウェアまたはコンテンツの利用者と前記複数のハードウェア情報または前記複数の利用者情報とをチェックし正当かどうか認証する機能を持つことを特徴とする請求項１に記載のコンテンツ共有管理システム。

【請求項３】　前記ハードウェア認証部または利用者認証部は、

認証の依頼を行い、返却された認証の結果を出力する第１の認証部分と、

コンテンツの所在場所と異なる場所に、コンテンツと利用者の対応と、コンテンツとハードウェアの対応の、どちらかまたは両方のコンテンツ利用管理データを持ち、

前記認証の依頼により前記コンテンツ利用管理データに基づいて認証を行い、認証の結果を前記第１の部分に返却する機能をもつ第２の認証部分とを、

有することを特徴とする請求項１または２に記載のコンテンツ共有管理システム。

【請求項４】　前記コンテンツ利用部は、

コンテンツの利用条件をコンテンツと共に保持し、それらを識別する機能を持つことを特徴とする請求項１から３までのいずれか１項に記載のコンテンツ共有管理システム。

【請求項５】　前記ハードウェア認証部、前記利用者認証部、前記利用条件判断部および前記利用条件更新部がサーバ上に存在し、

前記コンテンツ利用部は、コンテンツ利用の都度に、前記サーバに利用許諾を問い合わせることを特徴とする請求項１から４までのいずれか１項に記載のコンテンツ共有管理システム。

2

【請求項６】　ディジタルコンテンツ流通において、

そのコンテンツを利用することが許される利用者の情報と、そのコンテンツを利用することが許されるハードウェア環境の情報のどちらか、または、両方の情報と、コンテンツとを対応付けする過程と、

前記コンテンツを利用する際に、該コンテンツの利用者と利用ハードウェア環境のどちらか、または、両方が、該コンテンツに対応付けされた前記情報と比較し、許されている場合のみ該コンテンツを利用可能とする過程とを、

有することを特徴とするコンテンツ保護方法。

【請求項７】　前記対応付けする過程では、

前記コンテンツと前記利用者の情報または前記ハードウェア環境の情報との対応付けを、前記ハードウェアの情報または前記利用者の情報を元に作成した鍵により、前記コンテンツを暗号化することで実現することを特徴とする請求項６に記載のコンテンツ保護方法。

【請求項８】　前記対応付けする過程では、

コンテンツを利用することが許される利用者とハードウェアの、どちらかまたは両方が、複数存在することを特徴とする請求項６または７に記載のコンテンツ保護方法。

【請求項９】　ディジタルコンテンツ流通における、コンテンツ保護方法であって、

コンテンツの利用ハードウェアが正当かどうかを認証するハードウェア認証過程と、

コンテンツの利用者が正当かどうかを認証する利用者認証過程と、

前記認証の結果、正当な利用者による他のハードウェア上での利用、または、正当なハードウェア上での他利用者による利用である場合には、その利用がそのコンテンツにおいて許されているか否かを調べる利用条件判断過程と、

前記判断の結果、許される場合には、コンテンツの利用条件を利用可能になるように更新する利用条件更新過程と、

コンテンツに指定されたコンテンツ利用条件または前記更新されたコンテンツ利用条件に基づきコンテンツを利用するコンテンツ利用過程と、

有することを特徴とするコンテンツ保護方法。

【請求項１０】　前記コンテンツ利用条件は、あらかじめ複数の利用ハードウェア情報または複数の利用者情報を登録されたものであり、

前記ハードウェア認証過程または前記利用者認証過程では、コンテンツの利用ハードウェアまたはコンテンツの利用者と前記複数のハードウェア情報または前記複数の利用者情報とをチェックし正当かどうか認証することを特徴とする請求項９に記載のコンテンツ保護方法。

【請求項１１】　請求項６から１０までのいずれか１項に記載のコンテンツ保護方法における過程を１または複数のコンピュータで実行するためのプログラムを、該１または複数のコンピュータが読み取り可能な１または複数の記録媒体に記録したことを特徴とするコンテンツ保護方法を記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ディジタルコンテンツ流通における、コンテンツ保護および正当な複製利用に関するものである。

【０００２】

【従来の技術】ディジタルコンテンツの流通において、不正利用を避けるためのコンテンツ保護技術が検討されている。これらのコンテンツ保護は、専用のハードウェアを用い、その特定のハードウェア以外では、コンテンツが利用できないようにしていたり、汎用パソコンにおいては、許可する際にハードウェア上に情報を保存し、そのハードウェア上でのみコンテンツが利用できるようにしていたりする。いずれも、ハードウェアとコンテンツを括り付けているところが特徴である。

【０００３】

【発明が解決しようとする課題】ディジタルコンテンツ流通の中でも、プログラムコンテンツは、その利用条件として一つのハードウェアでの利用（インストール）のみ認められているものが多いが、コンテンツの正当な利用条件の中には、利用者による複製が許されている場合がある。例えば、画像コンテンツなどは、その利用者が使用する範囲では、一般に別ハードウェアであってもコピーが許されている。

【０００４】コンテンツの保護手段における、従来の方法では、複数のハードウェアを利用している場合、ハードウェアとコンテンツが対応付けられているため、利用者が正当な権利としてコピーしようとしても、利用許諾を受けたハードウェアと異なるハードウェアにおいては、コンテンツが利用できない。

【０００５】本発明は、この問題を解決すべく、正当な権利の範囲内において、利用者がコンテンツを複製するなど共有利用できる環境を提供することを課題とするものである。

【０００６】

【課題を解決するための手段】本発明は、以下に列記する手段により、上述の課題を解決する。

【０００７】その一手段は、ディジタルコンテンツ流通における、コンテンツ共有管理システムであって、コンテンツに指定されたコンテンツ利用条件または更新された利用条件に基づきコンテンツを利用するコンテンツ利用部と、コンテンツの利用ハードウェアが正当かどうかを認証するハードウェア認証部と、コンテンツの利用者が正当かどうかを認証する利用者認証部と、前記認証の結果、正当な利用者による他のハードウェア上での利用、または、正当なハードウェア上での他の利用者による利用である場合には、その利用がそのコンテンツにおいて許されているか否かを調べる利用条件判断部と、前記判断の結果、許されている場合には、コンテンツの利用条件を利用可能とするように更新する利用条件更新部とを、有することを特徴とするコンテンツ共有管理システムである。

【０００８】あるいは、前記コンテンツ利用条件に、あらかじめ複数の利用ハードウェア情報または複数の利用者情報を登録する機能手段を有し、前記ハードウェア認証部または前記利用者認証部は、コンテンツの利用ハードウェアまたはコンテンツの利用者と前記複数のハードウェア情報または前記複数の利用者情報とをチェックし正当かどうか認証する機能を持つことを特徴とする上記のコンテンツ共有管理システムである。

【０００９】あるいは、前記ハードウェア認証部または利用者認証部は、認証の依頼を行い、返却された認証の結果を出力する第１の認証部分と、コンテンツの所在場所と異なる場所に、コンテンツと利用者の対応と、コンテンツとハードウェアの対応の、どちらかまたは両方のコンテンツ利用管理データを持ち、前記認証の依頼により前記コンテンツ利用管理データに基づいて認証を行い、認証の結果を前記第１の部分に返却する機能をもつ第２の認証部分とを、有することを特徴とする上記のコンテンツ共有管理システムである。

【００１０】あるいは、前記コンテンツ利用部は、コンテンツの利用条件をコンテンツと共に保持し、それらを識別する機能を持つことを特徴とする上記のコンテンツ共有管理システムである。

【００１１】あるいは、前記ハードウェア認証部、前記利用者認証部、前記利用条件判断部および前記利用条件更新部がサーバ上に存在し、前記コンテンツ利用部は、コンテンツ利用の都度に、前記サーバに利用許諾を問い合わせることを特徴とするコンテンツ共有管理システムである。

【００１２】また、別の一手段は、ディジタルコンテンツ流通において、そのコンテンツを利用することが許される利用者の情報と、そのコンテンツを利用することが許されるハードウェア環境の情報のどちらか、または、両方の情報と、コンテンツとを対応付けする過程と、前記コンテンツを利用する際に、該コンテンツの利用者と利用ハードウェア環境のどちらか、または、両方が、該コンテンツに対応付けされた前記情報と比較し、許されている場合のみ該コンテンツを利用可能とする過程とを、有することを特徴とするコンテンツ保護方法である。

【００１３】あるいは、前記対応付けする過程では、前記コンテンツと前記利用者の情報または前記ハードウェア環境の情報との対応付けを、前記ハードウェアの情報

または前記利用者の情報を元に作成した鍵により、前記コンテンツを暗号化することで実現することを特徴とする上記のコンテンツ保護方法である。

【００１４】あるいは、前記対応付けする過程では、コンテンツを利用することが許される利用者とハードウェアの、どちらかまたは両方が、複数存在することを特徴とする上記のコンテンツ保護方法である。

【００１５】あるいは、ディジタルコンテンツ流通における、コンテンツ保護方法であって、コンテンツの利用ハードウェアが正当かどうかを認証するハードウェア認証過程と、コンテンツの利用者が正当かどうかを認証する利用者認証過程と、前記認証の結果、正当な利用者による他のハードウェア上での利用、または、正当なハードウェア上での他利用者による利用である場合には、その利用がそのコンテンツにおいて許されているか否かを調べる利用条件判断過程と、前記判断の結果、許される場合には、コンテンツの利用条件を利用可能になるように更新する利用条件更新過程と、コンテンツに指定されたコンテンツ利用条件または前記更新されたコンテンツ利用条件に基づきコンテンツを利用するコンテンツ利用過程と、有することを特徴とするコンテンツ保護方法である。

【００１６】あるいは、前記コンテンツ利用条件は、あらかじめ複数の利用ハードウェア情報または複数の利用者情報を登録されたものであり、前記ハードウェア認証過程または前記利用者認証過程では、コンテンツの利用ハードウェアまたはコンテンツの利用者と前記複数のハードウェア情報または前記複数の利用者情報とをチェックし正当かどうか認証することを特徴とする上記のコンテンツ保護方法である。

【００１７】あるいは、上記のコンテンツ保護方法における過程を１または複数のコンピュータで実行するためのプログラムを、該１または複数のコンピュータが読み取り可能な１または複数の記録媒体に記録したことを特徴とするコンテンツ保護方法を記録した記録媒体である。

【００１８】本発明では、コンテンツを利用しようとしたとき、利用条件に沿っているか否かを調べるために、必要に応じて、正当なハードウェアか否か、正当な利用者か否かを認証する。その順序は問わないが、どちらか一方または両方が正当でないと判断したとき、利用条件としてハードウェアや利用者の新たな許諾が許されているか否かを判断し、許されているなら、現在のハードウェア情報または利用者情報または両方を元に、利用可能なになるように利用条件を更新する。これにより、正当な利用条件の基に、異なるハードウェアでのコンテンツ共有等を可能にする。

【００１９】

【発明の実施の形態】以下、本発明の実施の形態を図示例と共に説明する。

【００２０】図１は、本発明のコンテンツ共有システムの一実施形態例の構成図を示す。コンテンツ利用部１は、コンテンツが利用されるハードウェア上にあり、他の部分を制御する。その他のハードウェア認証部２、利用者認証部３、利用条件判断部４、利用条件更新部５は、一部あるいはすべてが、コンテンツ利用管理データを保持しているコンテンツサーバ等に存在する場合がある。もちろん利用条件によって、これらの一部あるいはすべてを省略する場合も考えられる。

【００２１】本発明では、権利保護の仕組みとしてコンテンツとハードウェアが対応付けられている場合でも、他のハードウェア上において、利用者が正当な権利の基にそのコンテンツを用いる場合に、利用を可能とするもので、そのために、利用許諾されたハードウェアとコンテンツの対応付けを、別のハードウェアとコンテンツとの間でも対応付ける。コンテンツと利用者の対応についても同様である。

【００２２】コンテンツを利用しようとしたとき、利用条件に沿っているか否かを調べるために、必要に応じて、ハードウェア認証部２において正当なハードウェアか否かを、利用者認証部３において正当な利用者か否かを認証する。その順序は問わないが、どちらか一方または両方が正当でないと判断したとき、利用条件としてハードウェアや利用者の新たな許諾が許されているか否かを利用条件判断部４で判断し、許されているなら、利用条件更新部５において現在のハードウェア情報または利用者情報または両方を元に、利用条件を更新する。これにより、正当な利用条件の基に、異なるハードウェアでのコンテンツ共有等が可能になる。

【００２３】ハードウェアの情報としては、例えば、ネットワークカードのＭＡＣアドレスや、ハードディスクのボリューム番号の情報や、あるいは、そのハードウェアにおいて比較的変わらないものであれば、ＯＳ等、ソフトウェアのシリアル番号のような情報でもよい。利用者の情報としては、ユーザＩＤとパスワードや、メールアドレス、あるいは、ＩＣカードによる個人特定や、指紋認証、声紋認証、筆跡認証などから得られる情報等がある。ハードウェア情報、利用者情報とも、何を用いるかは、取得可能なものをシステムで決めておけば、何でも良い。ハードウェア情報は、プログラムが読み取る場合が多いが、利用者による入力も可能である。利用者情報は、ユーザＩＤとパスワード、メールアドレスなど、利用者が入力する場合が多いが、ＩＣカードや他の認証システムから利用者ＩＤ等の情報をプログラムが作成することも可能である。また、複数の情報を用いることもできる。

【００２４】コンテンツとこれらの情報との対応付けは、例えば、これらの情報とコンテンツを識別する情報を、単に表形式で保持しておく方法や、コンテンツの中に電子透かしなどで隠す方法がある。対応付けの方法と

して、共通鍵暗号方式の鍵として、ハードウェア情報または利用者情報を用い、コンテンツを暗号化する方法がある。暗号化はコンテンツ入手時にサーバ側で行うのが一般的であるため、これらの情報から特定の方法により鍵を作り、その鍵で暗号化する。これにより、復号する場合でも、直接鍵をやり取りすることなく、利用されるその環境から鍵が生成できる。

【００２５】ある利用者がコンテンツ入手時に、そのとき利用しているハードウェア以外に、他のハードウェア情報を投入することにより、複数のハードウェア情報のリストを作成する。あるいは、複数の利用者情報を投入することにより、利用者情報のリストを作成する。これを、それぞれの組み合わせの数だけ展開するか、または、このままリストとして用いて、コンテンツと対応付ける。展開して用いる場合は、一つの情報を用いる場合と同じである。

【００２６】コンテンツ入手時等、利用条件として、利用可能な複数のハードウェア情報のリストが設定された場合、ハードウェア認証部２において、複数のハードウェア情報の中に、現在利用しているハードウェアが存在するかどうかをチェックする機能を持つことで、あらかじめ定められた複数のハードウェア上でのコンテンツ共有が可能となる。利用者情報を複数もつ場合も同様である。

【００２７】コンテンツを管理するサーバが、コンテンツ利用管理データとして、コンテンツ配布先の利用者情報を保持し、利用者認証部３からの問い合わせに対して、例えば、利用者番号とメールアドレス、または、会員番号と暗証番号等により、利用者を認証し、結果を利用者認証部３へ返却することで、利用者の認証を行うことも可能である。ハードウェア情報の認証に対しても同様である。

【００２８】ここで、コンテンツ利用部１において、コンテンツ利用条件にある許諾された利用者情報と、許諾されたハードウェア情報を抽出し、利用者認証部３およびハードウェア認証部２にそれらのデータを渡すことにより、認証を行う。

【００２９】コンテンツ利用部１にコンテンツ管理サーバへの問い合わせ機能を持ち、利用の都度、サーバに利用許諾を問い合わせることも可能である。コンテンツ管理サーバは、それぞれのコンテンツ毎に、コンテンツ利用管理情報として、利用者とハードウェアの情報、および、コンテンツの利用条件を管理する。コンテンツ利用部１から利用許諾の問い合わせがあると、利用者の確認、ハードウェアの確認、コンテンツの利用条件により利用者情報やハードウェア情報の更新を行い、結果をコンテンツ利用部１へ回答する。処理の例としては、許諾条件の問い合わせにより、まず、許可された利用者かをチェックする。利用者が許されていなければ、コンテンツ利用部１に拒否を返す。利用者が許可されていれば、利用者に許されたハードウェアかどうかをチェックする。コンテンツの利用条件により別ハードウェアでの利用が可能で、ハードウェアが許されていなければ、ハードウェア情報を追加し、コンテンツ利用部１に許可を返す。

【００３０】図２は、本発明のコンテンツ共有管理システムの処理例とともに、本発明のコンテンツ保護方法の一実施形態例を示すフローチャートである。ここでは、従来技術の問題点をどの様に解決しているかを示す、最も特徴的な例を示す。すなわち、画像コンテンツを購入した場合のように、正当な利用者により、別ハードウェアに複製利用された場合を考える。

【００３１】まず、コンテンツ利用部１から、利用条件を抽出する。次に、従来技術同様、コンテンツ利用条件にあるハードウェア情報から利用可能なハードウェアか否かを、ハードウェア認証部２により認証し、利用可能なハードウェアであれば、コンテンツ利用部１に対し正常利用させる。利用可能なハードウェアでない場合には、利用条件判断部４により、他のハードウェアでの利用が許されているコンテンツか否かを判定する。許されていなければ、不正利用である。許されている場合、正当な利用者か否かを利用者認証部３により認証する。正当な利用者ではない場合、不正利用である。正当な利用者の場合、利用条件更新部５により、ハードウェア情報を基に、利用条件としてそのハードウェアでの利用を許すように更新する。その更新は、複数のハードウェア情報が存在することができる場合は、追加するが、許されない場合は、新しいハードウェア情報で置きかえる。

【００３２】この例では、最初のハードウェア認証で成功した場合は、そのままコンテンツ利用部１に対し正常利用させているが、さらに厳密な利用条件の場合は利用者認証も行う。

【００３３】図３は、その利用者認証を含む全体の処理フローで、これらの内の一部分を省略した形でも実現される。利用者認証とハードウェア認証の順序は問わない。ただし、別のハードウェアでも許可されるコンテンツを、悪意を持った不正な利用者が利用条件を変えてしまうのを防ぐために、利用条件更新部で更新する前に利用者認証を行っておく必要がある。

【００３４】すなわち、まず、コンテンツ利用部１から、利用条件を抽出する。次に、利用者情報から正当な利用者か否かを、利用者認証部３により認証する。正当な利用者であれば、コンテンツ利用条件にあるハードウェア情報から利用可能なハードウェアか否かを、ハードウェア認証部２により認証する。利用者認証部３において、正当な利用者でないとされた場合には、利用条件判断部４により、他の利用者が利用可能か否か判定する。許されていなければ、不正利用である。許されている場合には、利用条件更新部５により、利用条件として当該他の利用者の利用を許すように更新し、コンテンツ利用

条件にあるハードウェア情報から利用可能なハードウェアか否かを、ハードウェア認証部２により認証する。ハードウェア認証部２によりハードウェアが利用可能であれば、コンテンツ利用部１に対し正常利用させる。ハードウェア認証部２において、利用可能なハードウェアでないとされた場合には、利用条件判断部４により、他のハードウェアでの利用が許されているコンテンツか否かを判定する。許されていなければ、不正利用である。許されている場合、利用条件更新部５により、ハードウェア情報を基に、利用条件としてそのハードウェアでの利用を許すように更新し、コンテンツ利用部１に対し正常利用させる。利用条件更新部５での更新は、複数のハードウェア情報が存在することができる場合は、追加するが、許されない場合は、新しいハードウェア情報で置きかえる。

【００３５】図４は、ハードウェア情報または利用者情報を複数もつことができる場合の、ハードウェア情報を例にした、ハードウェア認証部２の処理フローである。

【００３６】まず、コンテンツの利用条件にある複数のハードウェア情報を分解する。その一つのハードウェア情報と、利用されようとしているハードウェア情報を比較し、一致していれば、利用可能であると認証する。不一致であれば、分解した次のハードウェア情報と利用されようとしているハードウェア情報を比較し、一致して利用可能と認証されるまで繰り返す。分解した全てのハードウェア情報と不一致であれば、利用不可能と判断する。

【００３７】利用者情報が複数の場合における、利用者認証部の処理フローも同様となる。この場合、ハードウェア情報は利用者情報に、利用可能は正当に、利用不可能は非正当に置き換える。

【００３８】図５は、コンテンツの利用者やハードウェアの情報をコンテンツ利用管理データとして、サーバで管理している場合の、利用者認証部３の処理フローである。ハードウェア認証部も同様である。

【００３９】まず、利用者認証部３１が、コンテンツ管理サーバ上にある利用者認証部３２に認証を依頼する。利用者認証部３２は、認証に必要な利用者情報を入手するとともに、そのコンテンツの使用を許可している利用者情報をコンテンツ利用管理データから抽出し、両者を比較してそのコンテンツの正当な利用者か否か確認する。確認の結果は、依頼元の利用者認証部３１に返却され、その利用者認証部３１は、その確認の結果により正当であれば利用可能（正当）を、正当でなければ利用不可能（非正当）を出力する。

【００４０】なお、ハードウェア認証部の場合には、利用者認証部はハードウェア認証部に、利用者情報はハードウェア情報に置き換える。

【００４１】図６は、コンテンツ利用の都度、コンテンツ利用管理データを管理しているサーバに利用許諾を問い合わせる場合の処理フローである。

【００４２】まず、コンテンツ利用部１から、コンテンツ利用管理データを管理しているサーバ６に、コンテンツの利用許諾を問い合わせる。これを受けてサーバ６は、利用コンテンツ、利用者情報、ハードウェア情報を入手する一方、コンテンツ利用管理データより、そのコンテンツの使用を許可している利用者情報およびハードウェア情報、さらに、他ハードウェアや利用者を許可できるか否かの利用条件を抽出する。次いで、入手した利用者情報、ハードウェア情報と抽出した利用条件を比較し、上述したと同様に、利用者認証、ハードウェア認証、利用条件判断、利用条件更新を行い、結果を問い合わせたコンテンツ利用部１に返却する。コンテンツ利用部１は、受け取った結果が当該コンテンツの利用が正当である場合にのみ、正常利用が可能となる。

【００４３】なお、本発明のコンテンツ共有管理システムおよびコンテンツ保護方法は、上述の図示例にのみ限定されるものではなく、本発明の要旨を逸脱しない範囲内において種々変更を加え得ることは勿論である。

【００４４】また、図１で示した装置各部の一部もしくは全部の機能を、コンピュータを用いて実現することができること、あるいは、図２、図３、図４、図５、図６で示した処理過程をコンピュータで実行することができることは言うまでもなく、コンピュータでその各部の機能を実現するためのプログラム、あるいは、コンピュータでその処理過程を実行するためのプログラムを、そのコンピュータが読み取り可能な記録媒体、例えば、ＦＤ（フロッピー（登録商標）ディスク）や、ＭＯ、ＲＯＭ、メモリカード、ＣＤ、ＤＶＤ、リムーバブルディスクなどに記録し、提供し、配布することが可能である。上記各部の一部が別のハードウェア上で機能する場合には、ハードウェア毎に、そのプログラムを別々の記録媒体に記録するようにしても良いし、全プログラムを一つの記録媒体に記録しておいて、ハードウェア毎に必要なプログラムを起動するようにしても良い。

【００４５】

【発明の効果】以上説明したように、本発明によれば、利用者が同じであればハードウェアは問わない等のように柔軟なコンテンツ利用条件に対応し、コンテンツ保護が実現できるという優れた効果を奏し得る。

【図面の簡単な説明】

【図１】本発明のコンテンツ共有管理システムの一実施形態例を示す構成図である。

【図２】本発明の一実施形態例を示す図であって、典型的な処理フロー例を示すフローチャートである。

【図３】本発明の別の実施形態例を示す図であって、全要素を含む処理フロー例を示すフローチャートである。

【図４】複数の許可情報を含む場合の、認証部および認証方法の一実施形態例での処理フローを示すフローチャートである。

11　　12

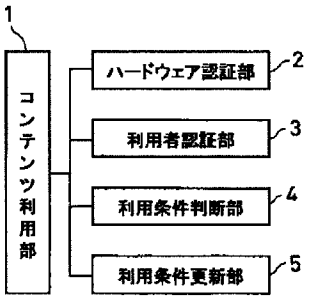
【図５】サーバで認証を行う場合の、本発明の一実施形態例を示す処理フローを示すフローチャートである。

【図６】コンテンツ利用の都度、サーバへ許諾確認を行う場合の、本発明の一実施形態例での処理フローを示すフローチャートである。

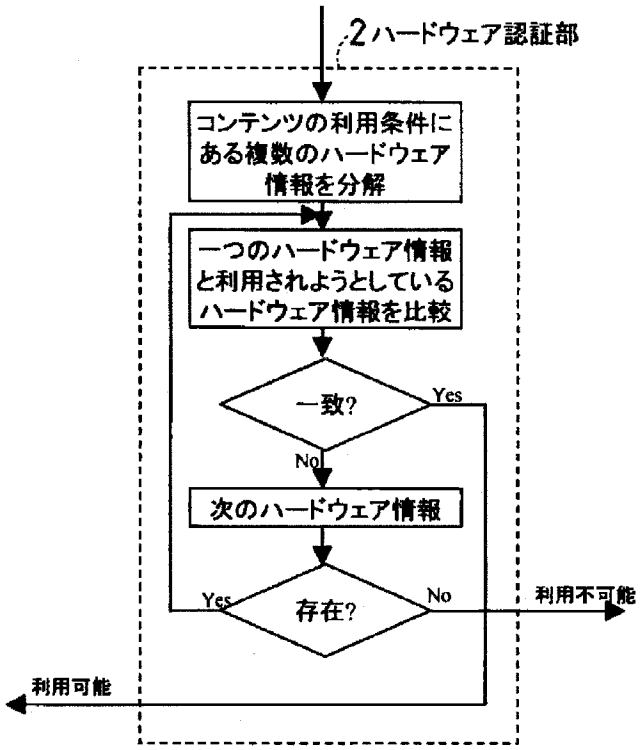
【符号の説明】

＊１…コンテンツ利用部
２…ハードウェア認証部
３…利用者認証部
４…利用条件判断部
５…利用条件更新部
＊６…コンテンツ利用管理データを管理しているサーバ

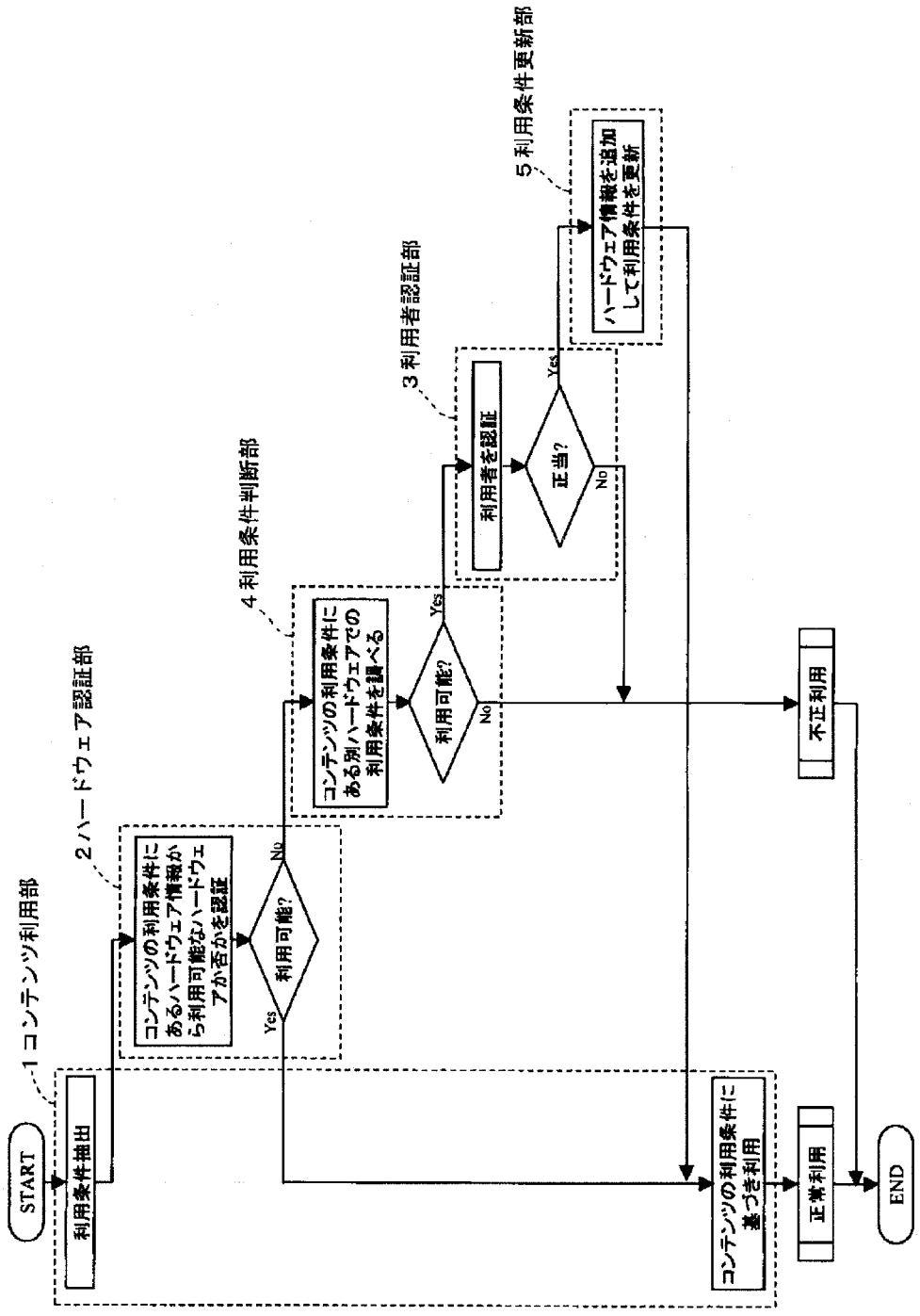
【図１】



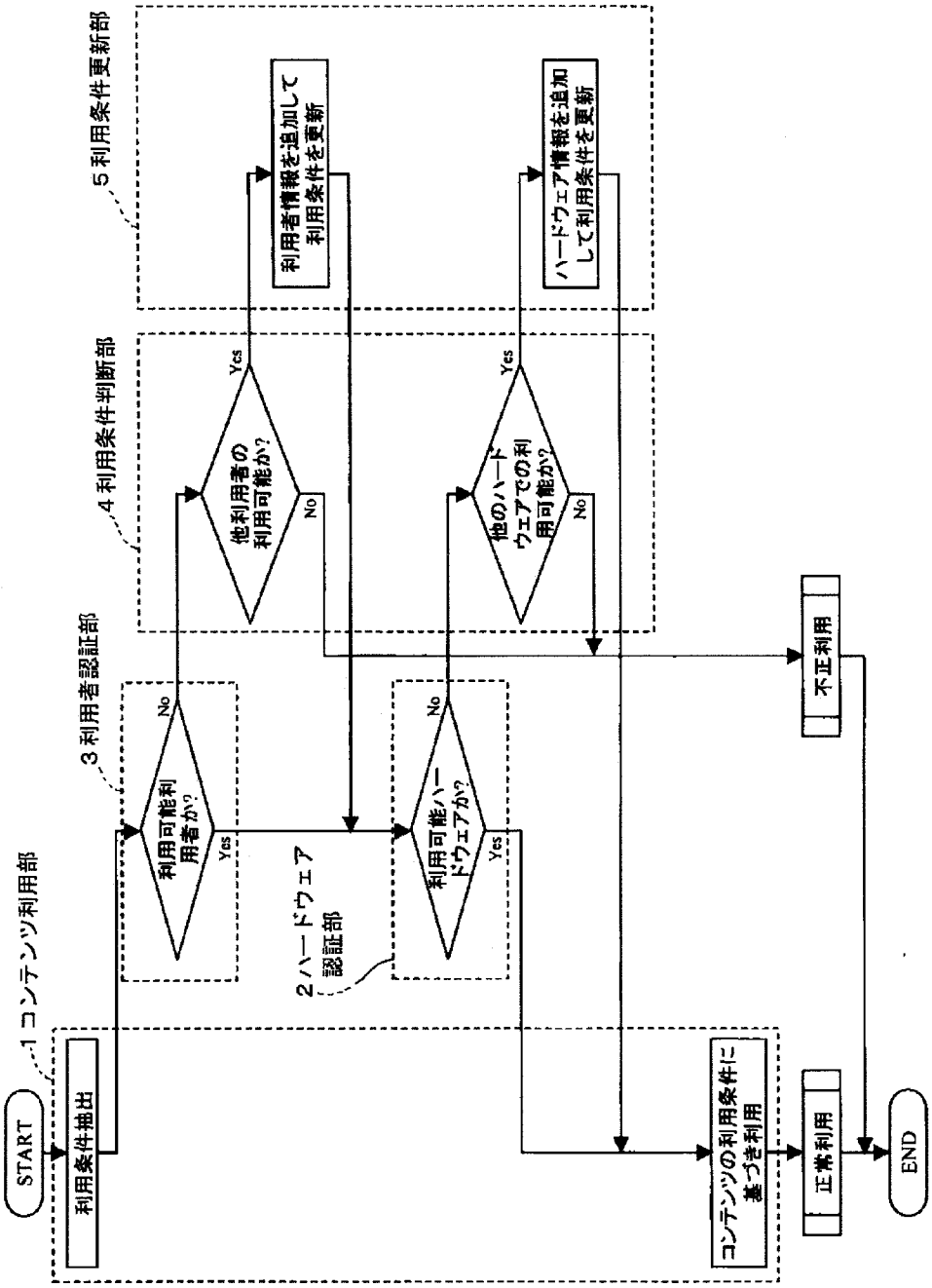
【図４】



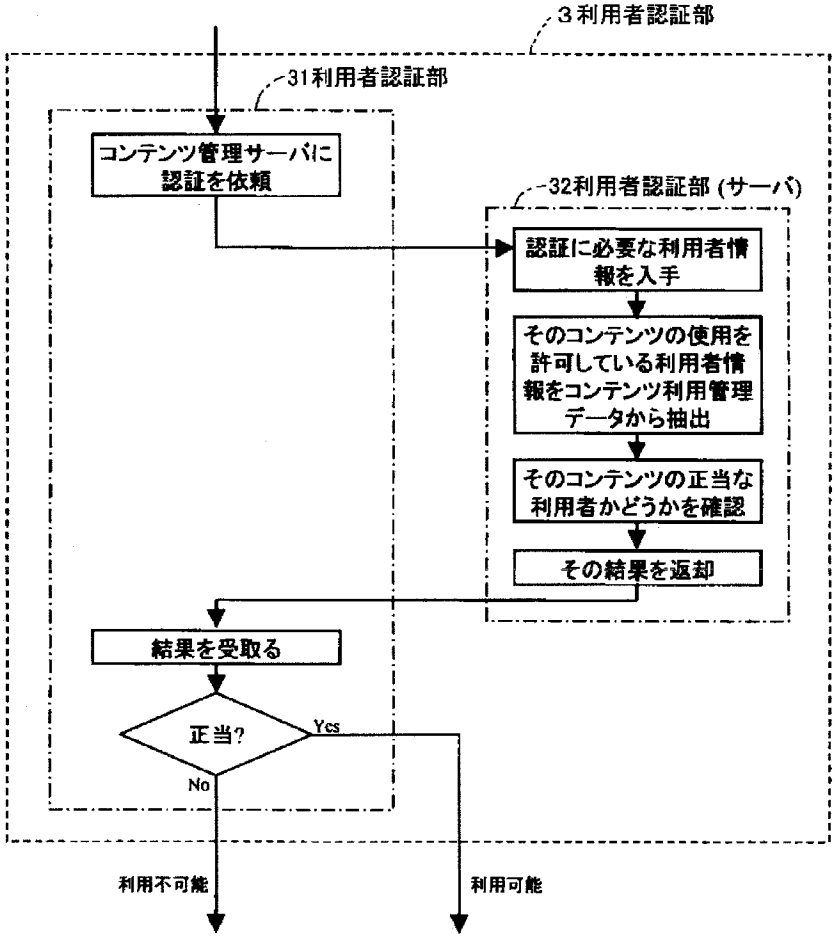
【図２】


START
1 コンテンツ利用部
利用条件抽出
2 ハードウェア認証部
コンテンツの利用条件にあるハードウェア情報から利用可能なハードウェアか否かを認証
利用可能?
No
Yes
4 利用条件判断部
コンテンツの利用条件にある別ハードウェアでの利用条件を調べる
利用可能?
Yes
No
3 利用者認証部
利用者を認証
正当?
Yes
No
5 利用条件更新部
ハードウェア情報を追加して利用条件を更新
不正利用
コンテンツの利用条件に基づき利用
正常利用
END

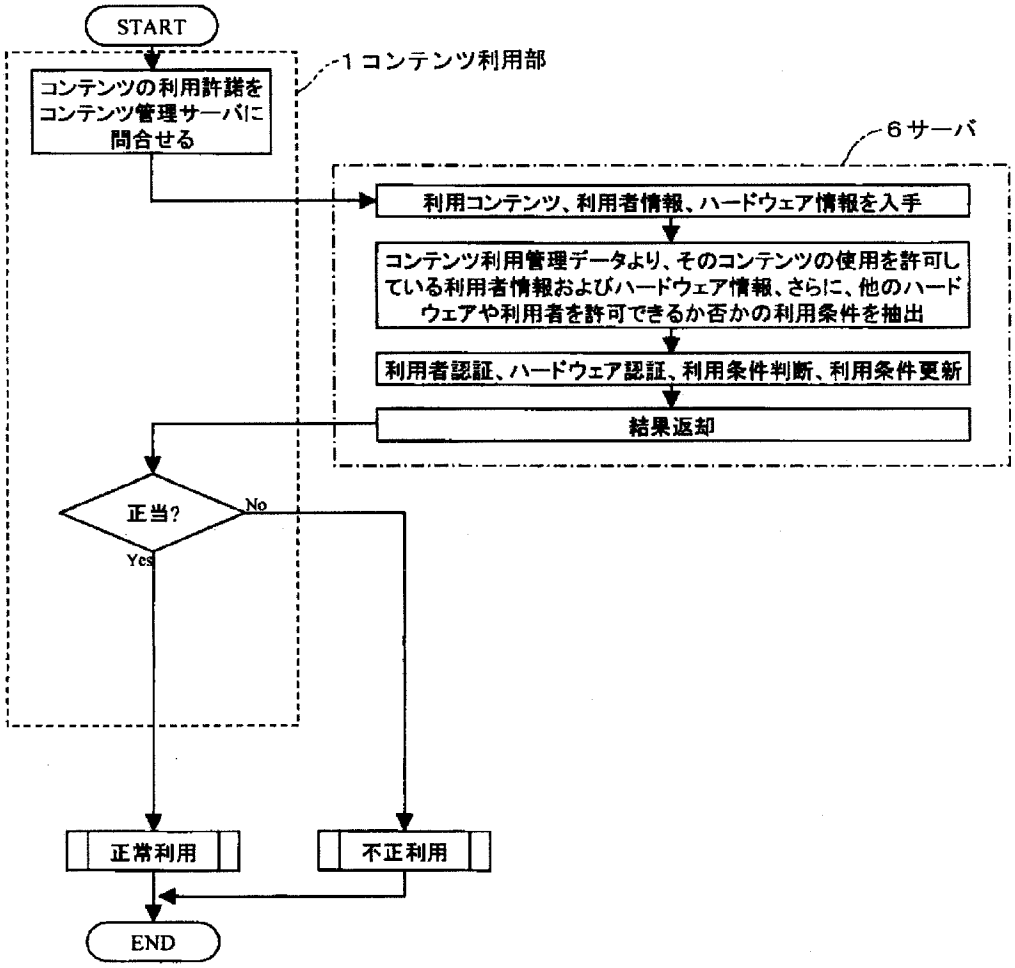
【図３】


START
1 コンテンツ利用部
利用条件抽出
3 利用者認証部
利用可能利用者か?
No
Yes
2 ハードウェア認証部
利用可能ハードウェアか?
No
Yes
4 利用条件判断部
他利用者の利用可能か?
Yes
No
他のハードウェアでの利用可能か?
Yes
No
5 利用条件更新部
利用者情報を追加して利用条件を更新
ハードウェア情報を追加して利用条件を更新
不正利用
コンテンツの利用条件に基づき利用
正常利用
END

【図５】


３利用者認証部
31利用者認証部
コンテンツ管理サーバに認証を依頼
32利用者認証部（サーバ）
認証に必要な利用者情報を入手
そのコンテンツの使用を許可している利用者情報をコンテンツ利用管理データから抽出
そのコンテンツの正当な利用者かどうかを確認
その結果を返却
結果を受取る
正当?
Yes
No
利用不可能
利用可能

【図６】



フロントページの続き

Ｆターム(参考)　5B017 AA04 AA07 BA05 BA07 BA09
BA10 BB10 CA07 CA08 CA09
CA12 CA14 CA15
5B076 FB01 FB06